



Department of Homeland Security Daily Open Source Infrastructure Report for 05 September 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The New York Times reports that the Transportation Security Administration, citing unexpected reliability problems, is suspending installation of the airport checkpoint device that automatically screens passengers for hidden explosives. (See item [10](#))
- Colorado State University engineering researchers have begun testing an early-warning security system designed to alert utility officials when major pollutants are detected in water supplies. (See item [21](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *September 01, Platts Energy Bulletin* — **Total strike will halt Nigerian oil exports.** Nigerian oil unions said Friday, September 1, oil exports from the West African country will be affected during the three-day strike planned for September 13. "The warning strike will affect downstream and upstream activities, onshore and offshore. There will be no oil exports during the period as we intend to make it total," said Peter Esele, president of the white-collar union Pengassan. The union resolved to stage the warning strike to protest against the government's failure and "lack of political will" to deal with the increasing violence and attacks on oil workers and installations in the Niger Delta. Nigeria, OPEC's sixth largest oil exporter, has

been struggling to curtail violence that erupted in the oil-rich Niger Delta since last January, which has cut over 25 percent of its oil production.

Source: <http://www.platts.com/Oil/News/8614356.xml?p=Oil/News&sub=Oil&src=energybulletin>

2. *August 31, Energy Central News* — **Iowa Falls company proposes wind farm project.**

Northern Iowa could have one of the nation's largest wind farms by 2008. Iowa Winds LLC wants to build a 200- to 300-megawatt farm covering about 40,000 acres in Franklin County. Iowa ranks third in the nation in wind energy behind Texas and California, according to the American Wind Energy Association. Company officials said the farm could be the nation's largest — depending on the permits and the county's power grid infrastructure. Iowa has nearly 900 wind turbines capable of producing 836 megawatts of electricity, enough to power about 226,000 average homes, according to the American Wind Energy Association.

Source: <http://www.energycentral.com/centers/news/daily/article.cfm?aid=7095227>

3. *August 30, VOA News* — **U.S. considers nuclear power to meet growing energy demands.**

As U.S. demand for energy continues to grow, a top American nuclear official says the United States is seriously considering stepping up its reliance on nuclear power. Nuclear power already accounts for 20 percent of the U.S. electricity supply. The last nuclear plant to open in the United States was 10 years ago. The new chairman of the Nuclear Regulatory Commission (NRC), Dale Klein, indicated that since U.S. demand for electricity remains strong, nuclear power generation is once again a serious option. According to Klein, nuclear power is an attractive option because "electrical demand is growing, concern on global warming and the unpredictability of fossil fuel costs." He said the NRC has received license applications from 16 different entities for 27 new nuclear power plants in the United States.

Source: <http://www.voanews.com/english/2006-08-30-voa55.cfm>

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

4. *September 01, Associated Press* — **Chemical spill prompts evacuations at Washington county dump.**

Residents near Newport, WA, were allowed to return to their homes Friday, September 1, after a chemical fire at a trash transfer station. Homeowners within a half-mile of the transfer station were evacuated and homeowners within a mile of the dump site were urged to keep their doors and windows closed.

Source: <http://www2.keprtv.com/x3442.xml?ParentPageID=x4192&ContentID=x45059&Layout=KEPR.xsl&AdGroupID=x3442&URL=http://localhost/apwirefeed/d8js7qh00.xml&NewsSection=StateHeadlines>

[[Return to top](#)]

Defense Industrial Base Sector

Nothing to report.

[[Return to top](#)]

Banking and Finance Sector

5. *September 01, VNUNet* — **Experts warn of devious phishing attacks.** Phishing attacks will use more sophisticated social engineering, targeting consumers for financial and identity theft and businesses for intellectual property theft. This is the main conclusion of the August 2006 global malware report released Friday, September 1, by security firm MessageLabs. The days of crude phishing e-mails which consumers have learned to spot are coming to a close, warns the report. Cyber-criminals are now developing personalized approaches that ape legitimate businesses' customer relationship management techniques, or "victim relationship management." "The latest wave of phishing attacks uses social engineering techniques by harvesting personal data from social networking sites like MySpace," said Mark Sunner, chief technical officer at MessageLabs.
Source: <http://www.vnunet.com/vnunet/news/2163387/phishing-sophisticated>
6. *September 01, Websense Security Labs* — **Multiple phishing alert: Santander Central Hispano, Monster job search engine, Fairwinds Credit Union.** Websense Security Labs has received reports of multiple new phishing attacks. One attack targets customers of Santander Central Hispano. Users receive a spoofed e-mail message claiming that, due to some technical problems on the bank portal last week, their account details will need to be verified. The e-mail provides a link to a phishing site. Another attack targets Monster job search engine. Users receive a spoofed e-mail message, which claims that their resume has been found on Monster.de. The e-mail alleges to come from a company called Sapphire Technologies. The e-mail asks the user to fill in an application form in order to complete the enrollment process. The offer includes a number of bonuses and a salary between three and four thousand dollars. The message provides a link to a phishing Website. Another attack targets Fairwinds Credit Union. Users receive a spoofed e-mail message claiming that Fairwinds Online has been upgraded, and that their account information must be verified to keep the online services secure. The e-mail provides a link to a phishing site that attempts to collect the user's account information.
Screen shots:
<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=599>
<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=600>
<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=601>
Source: <http://www.websense.com/securitylabs/alerts/>
7. *August 31, Carnegie Mellon University* — **Carnegie Mellon CyLab researchers create new system to address phishing fraud.** Carnegie Mellon University's CyLab researchers have developed a new anti-phishing tool to protect users from online transactions at fraudulent Websites. A research team led by Electrical and Computer Engineering Professor Adrian Perrig has created the Phoolproof Phishing Prevention system that protects users against all network-based attacks, even when they make mistakes. The innovative security system provides strong mutual authentication between the Web server and the user by leveraging a mobile device, such as the user's cell phone or PDA. The system is also designed to be easy for businesses to implement. "The mobile device acts like an electronic assistant, storing a secure bookmark and a cryptographic key for each of the user's online accounts," said Perrig.
For further detail: <http://sparrow.ece.cmu.edu/~parno/phishing/>

Source: http://www.cmu.edu/PR/releases06/060831_phishing.html

8. *August 30, Government Accountability Office* — **GAO–06–659: Information Security: Federal Reserve Needs to Address Treasury Auction Systems (Report)**. The Federal Reserve System's Federal Reserve Banks (FRB) serve as fiscal agents of the U.S. government when they are directed to do so by the Secretary of the Treasury. In this capacity, the FRBs operate and maintain several mainframe and distributed-based systems — including the systems that support the Department of the Treasury's auctions of marketable securities — on behalf of the department's Bureau of the Public Debt (BPD). Effective security controls over these systems are essential to ensure that sensitive and financial information is adequately protected from inadvertent or deliberate misuse, disclosure, or destruction. In support of its audit of BPD's fiscal year 2005 Schedule of Federal Debt, the Government Accountability Office (GAO) assessed the effectiveness of information system controls in protecting financial and sensitive auction information on key mainframe and distributed-based systems that the FRBs maintain and operate for BPD. To do this, GAO observed and tested FRBs' security controls. GAO is recommending that the Chairman, Board of Governors, establish an effective management structure for information security activities and a test environment for auction systems. In written comments on a draft of this report, the Federal Reserve generally agreed with the report.

Highlights: <http://www.gao.gov/highlights/d06659high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-659>

9. *August 30, Websense Security Labs* — **Multiple phishing alert: Alternatives Federal Credit Union, Bumiputra Commerce Bank, Banca FIDEURAM**. Websense Security Labs has received reports of multiple new phishing attacks. One attack targets customers of Alternatives Federal Credit Union. Users receive a spoofed e-mail message claiming that in order to fight money laundering, their account details need to be confirmed. The e-mail provides a link to a phishing site that attempts to collect the user's account information. In another attack targeting Bumiputra Commerce Bank, users receive a spoofed e-mail message claiming that maintenance is being performed and that their account details must be confirmed. The e-mail provides a link to a phishing site that attempts to collect the user's account information. In another attack targeting Banca FIDEURAM in Italy, users receive a spoofed e-mail message claiming that a software update is taking place and that this requires a verification of all account details. The URL provided in the e-mail is a link to a phishing site that attempts to collect users' account information, such as login details.

Screen shots:

<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=596>

<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=597>

<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=598>

Source: <http://www.websense.com/securitylabs/alerts/>

[[Return to top](#)]

Transportation and Border Security Sector

10. *September 03, New York Times* — **Screening tools slow to arrive in U.S. airports**. Citing unexpected reliability problems, the Transportation Security Administration (TSA) is

suspending installation of the airport checkpoint device that automatically screens passengers for hidden explosives. TSA is assessing whether to modify the trace-detection portals (nicknamed puffers because they blow air while searching for residue from explosives), upgrade them or wait until better devices are available. The machines were developed by Sandia National Laboratories in 1997 and manufactured by General Electric and Smiths Detection at a cost of about \$160,000 each. Since 2001, the TSA laboratory had worked to improve the devices, testing the prototypes to ensure they could detect explosives and withstand constant use in airports. Once in use—about 95 machines have been installed in 34 airports, far short of the 350 intended to be in place at 81 airports by the end of this year—the machines' limitations became more obvious. The portals do not include sensors for liquid explosives. And despite efforts to ensure reliability, the puffers too often broke down or had other performance problems perhaps because of dust and dirt at airports, Mr. Null, the TSA technology official, said.

Source: <http://www.nytimes.com/2006/09/03/us/03research.html?ei=5065&en=7683ad196d739c67&ex=1157860800&partner=MYWAY&pagewanted=print>

11. *September 01, Associated Press* — **Controllers say staff shortages are everywhere.** Air traffic controllers say they have to keep track of more airplanes with fewer people as the Federal Aviation Administration (FAA) tries to control costs for operating air traffic control facilities. The staff shortage has forced some controllers to handle double-duty — simultaneously directing airplanes on the ground and monitoring air traffic by radar, much like the solo air traffic controller in Lexington, KY, last weekend when a commuter plane crashed trying to take off on the wrong runway. While FAA acknowledges short-staffing at Lexington Blue Grass Airport and a handful of other small airports, air traffic controllers say the problem extends to major airports around the country and is compromising safety. Ruth Marlin, executive vice president for the National Air Traffic Controllers Association, said, "The FAA is short-staffed at O'Hare, Atlanta, and Dallas towers. If you don't have enough people, you either can't provide the service or can't maintain the safety margin." There are 1,081 fewer controllers now than three years ago. As of May, Chicago O'Hare had 52 controllers, though it's authorized to have 71; Atlanta had 39 on staff, though authorized for 55; and Dallas-Fort Worth has 48, though authorized for 59, according to a report aviation expert Darryl Jenkins prepared for the controllers association.

Source: http://www.usatoday.com/travel/news/2006-09-01-faa-cuts_x.htm

12. *September 01, Associated Press* — **Illinois to redo background checks on 500 Hazmat drivers.** The Illinois secretary of state's office says about 500 drivers will have to redo background checks and fingerprinting if they want to get licenses to transport hazardous materials. That's because the federal Transportation Security Administration found that some of those fingerprints were missing or unreadable. Secretary of state's office spokesperson Dave Druker said the problems have come up in the last couple of months with the private companies that handle the fingerprinting.

Source: <http://abclocal.go.com/wls/story?section=local&id=4510707>

13. *September 01, Associated Press* — **Plane fire in Iran kills up to 80 people.** A plane with 147 people on board skidded off the runway in northeastern Iran on Friday, September 1, and caught fire, killing as many as 80 people, state television reported. State TV said earlier that a tire had blown out as the Russian-made Tu-154 was landing in the city of Mashhad. A

spokesperson for Iran's Civil Aviation Organization, Reza Jafarzadeh, told the Associated Press that the death toll and the cause of the incident were not yet clear. State TV later said that the death toll was between 70 and 80 and that 50–60 passengers were evacuated from the aircraft. The flight run by Iran Airtour, which is affiliated to Iran's national air carrier, originated in Bandar Abbas in the south of the country. Some 12 million pilgrims visit Mashhad, about 620 miles northeast of Tehran, annually for its Shiite Islamic shrines.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/01/AR2006090100420.html>

14. *August 31, Department of Transportation* — **Department of Transportation proposes new safety requirements for rural low-stress and gathering pipelines in unusually sensitive areas.** Certain pipeline operators will have to meet new, more rigorous safety requirements, including cleaning and continuous monitoring, along more than 1,200 miles of pipelines under a proposed rulemaking announced on Thursday, August 31, by Acting Secretary of Department of Transportation Maria Cino. If the proposed rule is finalized, the Department would regulate additional pipelines that would pose a significant risk to human health and the environment. Cino noted that the proposed rule would prevent the kind of maintenance lapses that led to a partial shutdown of 22 miles of low-stress pipelines operated by BP in northern Alaska. Cino added that the proposed rule would impose requirements similar to those for high-pressure pipelines that already have added protections for drinking water, endangered species habitats and other areas defined as “unusually sensitive areas.” The proposed new rule will, for the first time, require companies that operate low-pressure pipelines in unusually sensitive areas, like Prudhoe Bay in Alaska, to comply with federal safety regulations similar to those applied to high-pressure pipelines, which are established by the Department of Transportation's Pipeline and Hazardous Materials Safety Administration.

Source: <http://www.dot.gov/affairs/phmsa0806.htm>

[[Return to top](#)]

Postal and Shipping Sector

Nothing to report.

[[Return to top](#)]

Agriculture Sector

15. *September 02, Reuters* — **Low-risk bird flu found in Pennsylvania ducks.** Mallard ducks in Pennsylvania have tested positive for a low-pathogenic strain of the H5N1 bird flu virus, the U.S. Agriculture and Interior departments said on Saturday, September 2, adding to cases detected recently in Maryland and Michigan. A strain of the H5N1 avian influenza virus was found in wild ducks sampled August 28 in Crawford County in northwestern Pennsylvania. The virus also has been found during the last month in Michigan and on Friday, September 1, in Maryland. A low-pathogenic strain, which produces less disease and mortality in birds than does a high-pathogenic version, poses no threat to humans.

Source: http://today.reuters.com/news/articlenews.aspx?type=domestic&News&storyID=2006-09-02T220613Z_01_WAT006224_RTRUKOC_0_US-BI

16. *September 01, Minnesota Ag Connection* — **Minnesota to test more herds for bovine tuberculosis.** The Board of Animal Health announced that in order for Minnesota to regain its accredited free status, additional tuberculosis (TB) testing throughout the state is required. Herds will be selected for testing based on criteria developed by the U.S. Department of Agriculture (USDA). The testing is being completed to assure the USDA and other states that TB is not present in Minnesota cattle. Herds selected to participate in this targeted TB testing will receive a letter in the next few weeks that outlines the entire testing process.
Source: <http://www.minnesotaagconnection.com/story-state.php?Id=802&yr=2006>
17. *August 31, Stop Soybean Rust News* — **Soybean rust found in sentinel plots in South Carolina.** Asian soybean rust was found in soybean sentinel plots in a second South Carolina county — Orangeburg — Monday, August 28 and Wednesday, August 30. This is the second location and county to have rust in South Carolina this year. Rust was found in Calhoun County August 17. There are now 37 counties and parishes in the U.S. with soybean rust in 2006 in seven states, including on soybeans in six of the states.
Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=933>

[[Return to top](#)]

Food Sector

Nothing to report.

[[Return to top](#)]

Water Sector

18. *September 03, St. Louis Post-Dispatch (MO)* — **Ameren reports more tritium leaks at Callaway nuclear plant.** Workers at the Callaway nuclear plant discovered leaks of radioactive tritium this summer. Most of the previous six leaks stemmed from pipe breaks of varying sizes between 1987 and 2005, according to records on file with the Missouri Department of Natural Resources and interviews with the plant's operator, St. Louis-based AmerenUE. The low levels of tritium found beneath nine pipeline manholes this year were traced to dripping air-release valves. Ameren is continuing to investigate the latest leaks to the pipeline, which runs cooling water and other waste from the plant, near Fulton, MO, to the Missouri River. So far, no tritium or other radionuclides have been detected in two rounds of testing on private wells that supply drinking water to 20 neighboring properties. Ameren said none of the leaks have threatened public health.
Source: <http://www.stltoday.com/stltoday/news/stories.nsf/stlouiscitycounty/story/E686311AD1312797862571DE004496A2?OpenDocument>
19. *August 31, KMSB (AZ)* — **Fake Tucson water employees.** Two men, posing as Tucson, AZ, Water employees, went to at least two homes in the Midvale Park area and told residents their water was contaminated. Tucson Water is warning their customers to watch out for them. Two Tucson Water Department uniforms were stolen from a Tucson Water employee's house.

Police are uncertain whether what happened in Midvale is connected to the uniform thefts.

Source: http://www.fox11az.com/news/topstories/stories/kmsb_20060830_dm_waterimposters.50cb1d74.html

20. *August 30, U.S. Food and Drug Administration* — **Spring water recalled.** Kinney Drugs, of Gouverneur, NY, announced it is implementing a voluntary recall by the manufacturer of all sizes of Kinney brand water with a sell by date between June 27, 2008 and August 4, 2008. Kinney Drugs removed the affected water from its shelves on August 23, 2006 and subsequently ordered it destroyed at store level. Extra warehouse stock of the affected water has been returned to the manufacturer. The water is being recalled due to bromate levels that exceed the U.S. Food and Drug Administration (FDA) standard. Based on information from the FDA and the New York State Department of Health, the level of bromate discovered is not a health risk in humans.

Source: http://www.fda.gov/oc/po/firmrecalls/kinney08_06.html

21. *August 24, Colorado State University* — **Water security warning system to be tested.** Colorado State University engineering researchers have begun testing an early-warning security system designed to alert utility officials when major pollutants are detected in water supplies. Researchers are working with city officials in Loveland and Fort Collins, CO, to test the technology on municipal water systems. Ralph Mullinix, director of Loveland Water and Power, said early warning systems are needed because water distribution systems are most vulnerable after the water leaves the treatment plant.

Source: http://newsinfo.colostate.edu/index.asp?url=news_item_display&news_item_id=48300849

[[Return to top](#)]

Public Health Sector

22. *September 04, Associated Press* — **New cases of bird flu detected in in Egypt.** New cases of domestic fowl with bird flu were found in Egypt last week, the Health Ministry said Monday, September 4, the first new cases to be reported in months. Health Ministry official Amr Qandil said four people suspected with symptoms of bird flu in the southern province of Sohag were tested negative and discharged from hospital. The new cases of birds with the lethal H5N1 strain of the virus were found in a village in Sohag, 215 miles south of Cairo, on Tuesday, August 29, and in Cairo on Thursday, August 31. All the birds in the areas nearby were culled.

Source: http://www.iht.com/articles/ap/2006/09/04/africa/ME_GEN_Egypt_Bird_Flu.php

23. *September 02, Associated Press* — **New tuberculosis strain detected in Africa.** A new, deadly strain of tuberculosis (TB) has killed 52 of 53 people infected in the last year in South Africa, the World Health Organization (WHO) said Friday, September 1. The strain was discovered in the Kwazulu-Natal region of South Africa, and is classified as extremely drug-resistant. Drugs from two of the six second-line medicines, used as a last line of defense against TB, proved ineffective against the new strain. "We are extremely worried about the issue of extreme drug resistance," said Paul Nunn, coordinator of the WHO's drug resistance department. "If countries don't have the diagnostic capacity to find these patients, they will die

without proper treatment." The WHO and its partners, including the South African Medical Research Council and the U.S. Centers for Disease Control and Prevention, planned a two-day meeting next week in South Africa to discuss the new TB strain in Africa, Nunn said.

TB information: <http://www.cdc.gov/nchstp/tb/default.htm>

Source: <http://www.cbsnews.com/stories/2006/09/02/ap/health/mainD8JS EJTO0.shtml>

24. *September 01, Associated Press* — **Mosquito-borne virus kills Massachusetts boy.** A nine-year-old boy from Middleborough, MA, 35 miles south of Boston, died Thursday, August 31, from eastern equine encephalitis (EEE). The death is the first so far this year in Massachusetts from the mosquito-borne virus. The child developed a fever August 18 and was hospitalized two days later. He died Thursday afternoon, said Christine Powers-Perry, a spokesperson for Children's Hospital in Boston. The boy could have contracted the virus as early as August 8, but probably got the virus the following week, according to state health officials. Two other people — a 52-year-old woman from Lakeville and a 23-year-old man from Acushnet — have contracted the virus this year. Four people have died in the state from the virus in the last four years.

EEE information: <http://www.cdc.gov/ncidod/dvbid/arbor/eeefact.htm>

Source: <http://www.cbsnews.com/stories/2006/09/01/health/main1959540 .shtml>

25. *September 01, Agence France-Presse* — **Nigeria reports more polio cases.** Nigerian authorities have reported a sharp rise in the number of polio cases despite a government immunization drive. A total of 784 cases of the disease were registered in 17 states at the end of July, the National Program on Immunization (NPI) said. In June the figures were 501 cases in 15 states, compared to 244 cases in 18 states for the same period in 2005, it said in a statement on Friday, September 1. The news came as the agency was preparing to launch another phase of its immunization drive between September 7 and 11. It said 11 northern states would be involved in the next immunization drive. Nigeria has the largest number of polio cases in the world, accounting for 80 percent of cases worldwide and 98 percent in Africa. Some northern states halted the polio immunization drive for 11 months in 2004 and 2005 when radical Muslim clerics claimed the polio vaccine was laced with substances that could render girls infertile as part of a U.S.-led plot. Despite the resumption of the campaign two years ago, Nigeria remains the epicenter of the transmission of the polio virus in the world.

Global Polio Eradication Initiative: <http://www.polioeradication.org/>

Source: http://news.yahoo.com/s/afp/20060901/hl_afp/nigeriahealthpol io_060901134005

26. *August 31, Associated Press* — **New York City issues 9/11 medical guidelines.** New York City health officials issued long-awaited guidelines Thursday, August 31, to help doctors detect and treat 9/11-related illnesses — medical advice considered crucial for hundreds of ground zero workers now scattered across the U.S. Since the 2001 terror attacks, thousands of firefighters, police officers, construction workers and volunteers who toiled at ground zero have been screened for a host of medical ailments, including severe lung disease and gastrointestinal problems. The guidelines could be vital in getting proper treatment for ground zero workers who have either relocated, or who came from elsewhere and must rely on doctors in other states who are unfamiliar with ground zero symptoms and the most effective treatments. The guidelines suggest particular questions to ask, tests to give and ways to treat the 9/11 patients. The medical guidelines, also known as a protocol, will be mailed to all doctors in New York and distributed elsewhere by the federal government.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/08/31/AR2006083100922.html>

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

Nothing to report.

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

27. *September 01, Sophos* — Top ten malware threats and hoaxes reported to Sophos in August 2006. Sophos has revealed the most prevalent malware threats and hoaxes causing problems for computer users around the world during August 2006. The report reveals little movement, with last month's four most prevalent pieces of malware retaining their positions. There are no new entries in August's chart and only one re-entry, the Mytob-E worm which last appeared in the chart in May 2005. This month's top two -- Netsky-P and Mytob-AS -- were also the most common in August 2005. Protection against Netsky-P has been available for more than two years, yet it remains the most widespread e-mail worm. Just one in 278 e-mails are now viral infected, a significant decrease to August 2005 when one in every 50 e-mails circulating were viral. The majority of the new threats were Trojan horses. See source for to view the full report.

Source: <http://www.sophos.com/pressoffice/news/articles/2006/09/top-ten-virus-august-2006.html>

28. *August 31, CNET News* — Uptick in Windows attacks reported. Several security experts are warning of increased cyberattacks targeting Windows PCs. The SANS Internet Storm Center, Symantec, McAfee and several other security companies are warning of a new worm that wriggles into Windows PCs by way of a security flaw for which Microsoft issued a patch with security bulletin MS06-040 on August 8. On Thursday, August 31, Symantec raised its ThreatCon to Level 2, which means an outbreak is expected. In an alert to customers, the company said it is seeing "ongoing and frequent attacks" that utilize the MS06-040 flaw. There are now six variants of malicious code that exploit the vulnerability, Symantec said. The SANS Internet Storm Center noted on its Website that several people had reported increased malicious activity. Microsoft, however, has not seen an increase in malicious activity associated with MS06-040.

Source: http://news.com.com/Uptick+in+Windows+attacks+reported/2100-7349_3-6111583.html?tag=cd.top

29.

August 31, VNUNet — **Error knocks out thousands of Spanish sites.** An error in Spain's central domain registry resulted in thousands of Websites being unavailable for two hours last week. A failed software update resulted in 400,000 sites being knocked offline on Tuesday, August 29. The error was due to a hardware fault and lasted just over an hour. The outage only affected Websites hosting their domains through Network Solutions. While Network Solutions had a backup system in place to ensure continued service in case of failures, it did not prevent the crash.

Source: <http://www.vnunet.com/vnunet/news/2163310/error-knocks-thousands-spanish>

Internet Alert Dashboard

Current Port Attacks	
Top 10 Target Ports	1026 (win-rpc), 445 (microsoft-ds), 32794 (---), 139 (netbios-ssn), 113 (auth), 25 (smtp), 80 (www), 6346 (gnutella-svc), 135 (epmap), 1433 (ms-sql-s)
Source: http://isc.incidents.org/top10.html ; Internet Storm Center	
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov .	
Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it-isac.org/ .	

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

30. *September 04, Associated Press* — Hundreds evacuated near Montana fire. A fire in south-central Montana has spread across 180,000 acres, or more than 280 square miles, since it was started by lightning on August 22. On Monday, September 4, it was only about 20 percent contained, authorities said. Fire officials feared that wind and warmer temperatures this week will create extreme fire conditions. About 265 homes were evacuated in just a few hours Sunday night on the western flank of the fast-moving blaze, Sweetgrass County Disaster and Emergency Services Coordinator Kerry O'Connell said. The fire was spreading actively on its southwest side Monday, fire information officer Char Fuller said. Some ranchers were rounding up cattle in the area. National Guard troops have staffed roadblocks restricting access to the fire area.

Source: http://www.forbes.com/infoimaging/feeds/ap/2006/09/04/ap2991_741.html

[\[Return to top\]](#)

General Sector

31. *September 03, Associated Press* — Police search Islamic school, London addresses after terror suspects arrested. Detectives searched an Islamic school and addresses across London on Sunday, September 3, following raids to round up a gang alleged to have run terrorist training camps in Britain, police said. A three-mile exclusion zone was set up around the school, a former convent near Crowborough, 40 miles south of London, as officers examined

the site. The Jameah Islameah School, set on several acres of grounds, had only nine pupils, according to a December 2005 government inspection report. Government officials said the London arrests were in connection with the alleged recruitment and radicalization of young British Muslims. The 14 men, aged between 17 and 48, were being questioned on suspicion of committing, preparing or instigating terrorist acts, police said. Charles Hendry, a lawmaker representing the area where the school is located, said the jailed radical cleric Abu Hamza al-Masri had visited the school with a group of followers. Al-Masri is serving a seven-year prison sentence for inciting his followers to kill non-Muslims.

Source: http://www.iht.com/articles/ap/2006/09/03/europe/EU_GEN_Britain_Terror_Arrests.php

[[Return to top](#)]

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.